IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT AUTHORIZING THE SEARCH OF TWO CELLULAR PHONES CURRENTLY IN ATF CUSTODY IN BALTIMORE, MARYLAND	**Case. No.** 1:21-mj-2872 TMD

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Terence Byrne, a Special Agent ("SA") with the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF"), being duly sworn, depose and state as follows:

1. I submit this affidavit in support of an application for a search warrant authorizing the search of two cellphones:

- A black Apple iPhone, bearing IMEI: 356466108739726 **(SUBJECT ELECTRONIC DEVICE 1),** and
- A black Samsung cellular telephone, bearing IMEI: 353325703541783 **(SUBJECT ELECTRONIC DEVICE 2)**.

(collectively the **SUBJECT ELECTRONIC DEVICES**), further described in Attachment A. the **SUBJECT ELECTRONIC DEVICES** are currently in the custody of ATF in Baltimore, Maryland.

2. The ATF and Anne Arundel County Police Department ("AAPD") are investigating Rodney PROCTOR for violation of 18 U.S.C. § 922(g)(1) (possession of a firearm and ammunition by a prohibited person) (the "Target Offense"). I submit that there is probable cause to believe that the **SUBJECT ELECTRONIC DEVICES**, further described in Attachment A, contain evidence of the Target Offense.

3. This affidavit is being submitted for the limited purpose of securing the requested warrant. I have not included details of every aspect of this investigation to date. Rather, I have set forth only those facts that I believe are necessary to establish probable cause supporting the warrant. I have not, however, intentionally omitted information that would tend to defeat a determination of probable cause. The information contained in this affidavit is based upon my personal knowledge, my review of documents, as well as conversations with other law enforcement officers and other individuals. All conversations and statements described in this affidavit are related in substance and in part unless otherwise indicated.

AFFIANT BACKGROUND

4. I am "an investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

5. Specifically, I am a Special Agent with ATF and am currently assigned to the Baltimore Field Division, Group VII, Crime Gun Enforcement Team. I have worked for ATF since November of 2017, and I attended the Department of Homeland Security's Criminal Investigator Training Program and ATF's Special Agent Basic Training for a combined period of 26 weeks, during which time I received extensive training in the provisions of firearms and narcotics laws administered under Title 18, Title 21, and Title 26 of the United States Code. Prior to my employment with ATF, I was employed by the Virginia Department of State Police as a State Trooper and Special Agent for six and a half years. I have participated in numerous investigations concerning the illegal possession and use of firearms, armed robbery, and violation of federal controlled substance laws. I have also received specialized and/or experiential training

on firearms, armed robbery, and controlled substance offenses, and personally participated in various types of investigative activities in connection with investigations into these offenses.

6. As a Special Agent, I have participated in complex investigations focusing on controlled dangerous substances ("CDS") trafficking, gangs, and illegal firearms. I have investigated people who illegally possess or traffic firearms, participated in the execution of state and federal search and arrest warrants involving violent offenders, and participated in the seizure of numerous firearms and CDS. Through my training and experience, I have become familiar with the manner in which illegal firearms are possessed, used, transported, stored, and distributed, the methods of payment for such, and the manner in which those who unlawfully possess and use firearms communicate with each other. Specifically, based upon my training and experience, I have learned the following:

a. Cellular telephones are an indispensable tool to those who unlawfully possess and use illegal firearms. These individuals use cellular telephones, push-to-talk telephones, Short Message Service ("SMS"), electronic-mail, and similar electronic means and/or devices, often under fictitious names or names other than their own, in order to maintain contact with other conspirators. Thus, these electronic devices hold valuable evidence of conversations between suspects regarding the unlawful possession and use of firearms;

b. Individuals who unlawfully possess and/or use firearms also use cellular devices to maintain records of their illegal activities, including telephone number "contact lists," address lists, photographs of firearms, and other personal identifiable information or information related to individuals who may have assisted in the purchasing and storage of firearms and ammunition; and

c. Individuals who unlawfully possess and/or use firearms use cellular telephones, pagers and other electronic communications devices to facilitate illegal transactions and keep in contact with co-conspirators. The electronically stored information on these devices is of evidentiary value in identifying other members of the conspiracy and establishing the relationship between these individuals, including photographs, texts, social media messages, and other identifying information stored on these devices.

PROBABLE CAUSE

7. On August 22, 2021, AAPD officers observed a gold Lexus pull into the turnaround circle in front of the Clarion Hotel, located at 7253 Parkway Drive, Hanover, Maryland. AAPD officers noticed the car's windows were heavily tinted and believed, through their training and experience, that the window tint was above the legal limit, so they initiated a traffic stop.[1]

8. The officers approached the driver's side window, identified the driver as Rodney PROCTOR, and immediately smelled a strong odor of marijuana emanating from the car. They asked PROCTOR if he had been smoking marijuana, and PROCTOR said that he and his friends had been partying the night before. The officers asked PROCTOR to get out of the car so they could search it. While PROCTOR was getting out, an officer observed a bulge in his front pant pocket, so he frisked him, but he did not find any contraband.

9. During the search of PROCTOR's car, officers located a black Taurus G3C 9mm pistol bearing serial number ABM215183 that was loaded with 10 rounds of 9mm ammunition under the front driver's seat. They also found multiple bags of suspected marijuana that weighed approximately 178 grams in total, drug paraphernalia with suspected marijuana residue, a black lid to a digital scale, $819.00, and **SUBJECT ELECTRONIC DEVICE 2**. Officers subsequently searched PROCTOR and found **SUBJECT ELECTRONIC DEVICE 1**.

10. The firearm was later test fired and determined to be operable, thereby satisfying the definition of a firearm pursuant to 18 U.S.C. § 921. The firearm was manufactured outside the state of Maryland and traveled in interstate commerce prior to its recovery in Maryland.

[1] Officers later confirmed the window tint was above the legal limit by using a tint meter, which is a machine designed to measure the tint percentage.

11. Further investigation revealed that PROCTOR has been convicted of a crime punishable by imprisonment for a term exceeding one year. Specifically, in 2013, PROCTOR was convicted of a Hobbs Act Robbery and sentenced to 11 years imprisonment. Accordingly, at the time PROCTOR possessed the handgun on August 22, he was prohibited from possessing a firearm and knew or should have known that he had been convicted of a crime punishable by over a year imprisonment.

FORENSIC ANALYSIS OF ELECTRONIC COMMUNICATIONS DEVICES

12. Based on my training and experience, I know that electronic devices such as cellular phones (smartphones) can store information for long periods of time. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the **SUBJECT ELECTRONIC DEVICES** may still be stored on those devices, for various reasons, as discussed in the following paragraphs.

13. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT ELECTRONIC DEVICES** were used, the purpose of their use, who used them, and when.

14. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT ELECTRONIC DEVICES** because data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs

store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

15. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

16. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

17. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

18. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. Again, the **SUBJECT ELECTRONIC DEVICES** remain in the custody of law enforcement. The only known specifics of each phone requested for authorization to search are

detailed in Attachment A and the types of information expected to be recovered from the devices are listed in Attachment B.

CONCLUSION

20. WHEREFORE, I respectfully request that this Court issue a warrant to search the **SUBJECT ELECTRONIC DEVICES**, further described in Attachment A, for certain evidence and information, further described in Attachment B and herein.

21. Additionally, I believe there is good cause to authorize the requested searches at any time of the day or night. The **SUBJECT ELECTRONIC DEVICES** are already in law enforcement custody, and it is reasonable to allow law enforcement to execute the requested searches at any hour of the day, even during the evening or night, if doing so is convenient for the investigators or examiners. Because the devices are in law enforcement custody already, there is no prejudice to any other person from this request.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

TERENCE BYRNE

Digitally signed by TERENCE BYRNE
Date: 2021.10.14 13:27:39 -04'00'

Terence O. Byrne III, Special Agent
Bureau of Alcohol, Tobacco, Firearms, and Explosives

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 15 day of October, 2021.

The Honorable Thomas M. DiGirolamo
United States Magistrate Judge

ATTACHMENT A
Items to be Searched

The **SUBJECT ELECTRONIC DEVICES**,

- One (1) black Apple IPhone, bearing IMEI: 356466108739726 **(SUBJECT ELECTRONIC DEVICE 1)**; and
- One (1) black Samsung cellular telephone, bearing IMEI: 353325703541783 **(SUBJECT ELECTRONIC DEVICE 2)**;

which are currently in the custody of ATF in Baltimore, Maryland.

ATTACHMENT B
Items to be Seized

All records contained in the items described in Attachment A, which constitute evidence of violations of the Target Offense including but not limited to that outlined below:

1. Contact logs that refer or relate to the user of any and all numbers on the **SUBJECT ELECTRONIC DEVICES**.

2. Call logs reflecting date and time of received calls.

3. Any and all digital images and videos of persons associated with this investigation.

4. Text messages to and from the **SUBJECT ELECTRONIC DEVICES** that refer or relate to the crimes under investigation.

5. Records of incoming and outgoing voice communications that refer or relate to the crimes under investigation.

6. Voicemails that refer or relate to the crimes under investigation.

7. Voice recordings that refer or relate to the crimes under investigation.

8. Any data reflecting the phone's location.

9. Contact lists.

10. Any and all records related to the location of the user(s) of the devices.

11. For the **SUBJECT ELECTRONIC DEVICES**:
    a. Evidence of who used, owned, or controlled the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;
    d. evidence of the attachment to the of **SUBJECT ELECTRONIC DEVICES** other storage devices or similar containers for electronic evidence;
    e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT ELECTRONIC DEVICES**;
    f. evidence of the times the **SUBJECT ELECTRONIC DEVICES** was used;
    g. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT ELECTRONIC DEVICES**;

h. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the; **SUBJECT ELECTRONIC DEVICES** and,
i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

2. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

3. "scanning" storage areas to discover and possible recover recently deleted files;

4. "scanning" storage areas for deliberately hidden files; or

5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The

investigative team will take no further steps regarding any review of information so segregated, absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.